IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Impact of Artificial Intelligence on Cybercrime –

-Keshav Pani, BA LLB , Christ University

Abstract : In the advent of GenAI becoming popular a few months ago and with the AI traditional paths becoming now a mainstream embed in many retail, payment ,and other productivity journeys, Frauds using AI like Deepfake Videos, Audio similarities and cloning the voice, AI for payment traps has become more frequent and popular. AI now can be seen by both – the hackers/fraudsters as well as the Cyber security defence team. It is important to gauge the impact of AI in this space and this papers gives a point of view of the same.

Introduction:- Artificial intelligence is where a machine(especially a gadget) copies human intelligence and functions with the incorporation of human of human intelligence. If artificial intelligence is used in the field of cybersecurity, cybersecurity will improve drastically but at the same time cybercrimes are tougher to track down when artificial intelligence is used to commit a cybercrime. Cybersecurity improved with the advent of Artificial intelligence because with application of human intelligence machines will detect cybersecurity threats quickly and even cyberthreats which are hard to detect or unlikely to be detected. However Artificial intelligence is used to commit cybercrimes. Example:- deepfake incidents in India. Main aim of this paper is to give information about the impact(good impact and bad impact) of artificial intelligence on cybersecurity , Assess bigger threat due to AI- enabled attacks and propose strategies to protect against future hacker threats. Objective of this paper is to tell the benefits of AI and the flaws of AI and how AI can be used in a judicious manner.

Method:- The methodology section outline the plan and method of how the study is conducted. This includes Universe of the study, sample of the study,Data and Sources of Data, study's variables and analytical framework. The details are as follows;

Population and Sample

The population sample of cases is small as it is an emerging area though relevant to all of us

Data and Sources of Data

For this study secondary data has been collected. I went through internet sources and different news articles to gather information about impact of Artificial intelligence on cybercrime. The news articles gave me information about different deepfake incidents. Also went through recent articles of Cybercrime Incidents that have been reported. The population sample is small as this is an emerging area though relevant to all of us.

Result:- In recent times , artificial intelligence has made it easier for functioning of several crime branches including cybersecurity .Artificial intelligence can improve cybersecurity. Security breach can be be detected quickly. Artificial Intelligence offered variety of tools and techniques that would boost cybersecurity defence . However hackers found it easier to hack and steal information. This research paper tells about how such threats to cyber security can be dealt with.

Hackers can leverage Artificial intelligence algorithms to develop more sophisticated malware that evades traditional cybersecurity defences and adapts to target specific vulnerabilities.

Deepfake is where someone's behaviour (especially voice) is imitated for entertainment purpose but deepfake is sometimes done due to malicious intent sometimes.

Deepfake technology can be used to create manipulated videos or audio recordings for social engineering attacks, fraud schemes and political manipulation. Artificial intelligence is used to do surveillance when not needed , people find it easier to initiate identity theft (take credit for a creative activity done by somebody else). Experts say that attackers can use generative AI and large language models to scale attacks at an unseen level of speed and complexity.

If machines are powered with artificial intelligence , there should be a mechanism to protect the machines even from AI-based attacks.

Discussion :- Introduction of artificial intelligence introduces new challenges like attack on individuals using Artificial Intelligence. Organisations should invest in cybersecurity solution, conduct security awareness training and collaborate with cyber security experts to enhance cyber resilience.

AI ethical guidelines , cybersecurity standards and data privacy regulations should be complied with.

. In recent times , artificial intelligence has made it easier for functioning of several crime branches including cybersecurity .Artificial Intelligence offered variety of tools and techniques that would boost cybersecurity defence . However hacker found it easier to hack and steal information. This research paper tells about how such threats to cyber security can be dealt with.

Deepfake has been used by hackers many times in India

In Uttar Pradesh , Accused impersonated face and voice of a former ips officer and threatened a senior citizen. The accused(while impersonating himself as a retired ips officer) said to the victim that if he did not deposit 74,000 rupees to accused then victim will be imprisoned for fake cases. Police took and help of cybersecurity and found the accused and booked the accused with relevant section 384 of Indian Penal Code(criminal intimidation) , section 378 ipc (stealing) and section 66D of Information Technology act2000 (which criminalises cheating through an electronic gadget) 1

A man called the victim and asked for money for daughter's surgery. The scammer claimed to be the victim's former colleague. The victim did a video call and the man was still moving his tongue like a normal man . The victim lied that he had insufficient balance . The victim called again and the accused spoke quickly which raised suspicion in the mind of victim of whether the guy who asked for help was really victim's former colleague. Victim called his former colleague who said that he(former colleague) never asked for help. 2

A gaming app promoted business through a fake AI generated video which showed that Akshay Kumar promoted the gaming app. Cyber-complaint was lodged against the gaming app as per section 66 D of IT Act which criminalises impersonation , especially in a technological device 5

A deepfake video featuring a popular cricketer Virat Kohli promoting betting went viral even though Virat Kohli does not endorse betting.

Cybercrime has adversely affected people in their daily lives. Examples :- data breach , , identity theft , phishing scams, etc.

Artificial technique tools are revolutionising the field of cybersecurity by providing tools and capabilities to enhance threat detection , incident response and risk assessment. One of the key techniques used in cybersecurity is machine learning (mechanism where an ai machine can imitate human behaviour) which enables the computers to learn from data and make intelligent decisions without explicit programming. Machine learning can programme large datasets to identify patterns, threats, anomalies or any sign of cyberthreat. This way ,Artificial Intelligence improves the mechanism of tackling breach of cybersecurity. Neural network is where data is processed the way data is processed in human body. Neural networks are enabled to recognise complex patterns and relationships in data , enabling them to detect subtle signs of malicious activities such as insider threats or advanced persistent threats. Neural network ensures that data is processed in a speedy manner. If people and entities start using neural network then decision can be made in a smooth manner also . Such entities can also enhance their capabilities of being faster and accurate in the field of detection of cyberthreat.

In Machine learning and neural network human mind is imitated. In Machine learning method , decision is made based on the data gathered whereas in neural network , procedures to operate is initiated in such a manner it can take decision on it's own.

Another Artificial intelligence technique in the field of cybersecurity which is becoming popular is natural language processing(where human language can be understood). Natural language processing gives machines the capability to understand and interpret human language. NLP algorithms can analyse unstructured data sources like emails, chat logs and social media content to detect potential cybersecurity threats or viruses . Example:- phishing is a virus that threatens cybersecurity or other cyber security risk that threatens cyber security like social engineering attack. By extracting required insights from text data, NLP Algorithms can improve threat intelligence mechanism and ensure faster response to cyber- incidents.

Anomaly detection a subset of AI approaches are essential for identifying any differences in the pattern in the way the machines function. Anomaly detection algorithms can detect and issue alert of any unusual activities(if there are any) or any event that may show a sign of security breach or any event that may cause security breach such as unauthorised access attempts , , unusual traffic patterns or unusual behaviour in the user.

In addition to Artificial Intelligence techniques predictive analysis plays a very important role in cybersecurity by predicting potential threats and vulnerabilities based on historical data patterns.

Internet of Things uses artificial intelligence to ensure cybersecurity. Artificial intelligence has boosted the cybersecurity mechanism in internet of things. 3

Machines should be designed with AI to prevent all sorts of cyberattacks(including AI driven attacks)

Intrusion detection system detects even slight intrusion of malicious traffic. However harmless data may be declared malicious and is blocked . A better solution needs to be found out to prevent AI-driven cyberattack and at the same time prevent inconvenience to technology users 4

Some countries have made laws to regulate the usage of artificial intelligence so that artificial intelligence is not misused. China has introduced laws to regulate Artificial Intelligence. Even European Union has brought up a law(binding on member-states) to regulate AI. European Union passed AI act (main aim of the act is to prevent misuse of AI) . However there is no law to regulate AI in countries like Britain, Japan, etc. There is no specific law in India to regulate AI. Section 420 of IPC punishes people who cheat others and get property that belongs to others. Section66 of IT Act2000 criminalises hacking where those doing hacking will be punished upto 3 years.

88 % of cybersecurity professionals are under the opinion that artificial intelligence can enhance cybersecurity to a huge extent and make cybersecurity efficient whereas 71% of cybersecurity professionals think that artificial intelligence would endanger cybersecurity because hackers will find it easier to hack. 61% of businesses believe that it is impossible to detect a breach without AI technology.69% of Information Technology experts believe that Artificial Intelligence is required to respond to future cyberattacks.7

Relevant Law Links : The laws around Cybercrime are still elementary in most countries. Intellectual Property rights area is being grappled. Guidelines are emerging and laws are still to strengthen. Data Privacy and protection acts have been tabled in India and should soon be formalised post elections (2024). An advisory dated May 9, 2023 has sounded a precautionary alarm against the possible adversarial threats that may arise from the use of AI language-based applications such as ChatGPT and Bard. Section 43A of the Information Technology Act 2000 (IT Act) states that a business handling 'any sensitive personal data or information' negligent in implementing and maintaining 'reasonable security practices and procedures' may be liable to pay compensation to an affected person and as per rule 8 of the Information Technology Rules, 2011, 'reasonable security practices and procedures' are considered to be complied if the business has implemented such security practices and standards as they are commensurate with the information assets being protected with the nature of the business. These will have to be strengthened specific to AI in the coming months.8

Conclusion

Introducing artificial intelligence in the field of cybersecurity would improve cybersecurity to a huge extent and threats by malicious actors who misuse technology can be contained . Detection of threats can be done in a better manner. Also defence mechanism can be enhanced and there is greater agility and effectiveness to respond to cyber incidents. However

it is essential to address ethical , legal and regulatory challenges associated with application of AI in the field of cyber security. By staying informed about the evolving threat landscape and implementing proactive security measures, organisations can strengthen their resilience against AI-Enabled attacks and safeguard their critical assets and data.

REFERENCES:-

1 India today.in - Cybercrime – Deepfake Incidents

2 Livemint - Deepfake and other cybercrime incidents

3Link.springer.com

4 Edgelabs.ai – AI role in cybercrime

5 times of india – Cybercrime Incidents

6 business today – Cybcercrime references

7 gitnux . org

8. cnbctv18.com – Cyber law references